

The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

MAURICIO A. LEON, M.D.,

Plaintiff,

v.

IDX SYSTEMS CORPORATION, a
Vermont Corporation,

Defendant.

No. CV03-1158P

DECLARATION OF HOWARD J.
BUNZEY IN SUPPORT OF
DEFENDANT'S MOTION RE:
SPOILIATION

I, Howard J. Bunzey, declare and say:

1. I am employed by the Defendant, IDX Systems Corporation as an Information Security specialist at its Vermont headquarters. I have personal knowledge of the matters stated herein.
2. IDX issued a Dell Latitude Laptop computer, model C600, Service Tag 1ZP5G01, to Dr. Mauricio Leon on April 4, 2001.
3. IDX maintains a "ticket" system for tracking the possession and maintenance of all computers issued to its employees. Under this system, employees requesting technical assistance submit a ticket to the Information Systems department, and the service dates the assistance is provided is logged. This system also indicates the issue and return date (if

any) for individual computers and any dates the laptop is upgraded or otherwise maintained by IDX.

4. My department reviewed the tracking system log for the laptop computer issued to Dr. Leon. The review indicated that a ticket was created on March 12, 2001 for the purchase, configuration and delivery of the laptop to Dr. Leon as a new hire. The ticket was completed and closed on April 4, 2001, when the laptop was delivered to Dr. Leon. Aside from this ticket, there were no other tickets for the laptop issued to Dr. Leon, which indicates that the laptop has never been returned to IDX's computer services department for any reason, including service or maintenance, since it was issued to Dr. Leon.

5. IDX has a computer use policy. General provisions of IDX's computer use policy provide: (1) all information technology resources must be used in accordance with all IDX policies; (2) information technology resources may not be used for entertainment; (3) installation of personal software on IDX systems is not allowed. IDX's Internet use policy prohibits accessing or sending of sexually oriented messages or images of any kind. In addition, IDX's Employee Guide provides that employees may not view or change electronic information that they are not authorized to access or modify. Attached to this Declaration as Exhibit A are true and correct excerpts from IDX's policies where these provisions are found.

I certify under penalty of perjury under the laws of the State of Vermont that the foregoing is true and correct.

DATED this the 27th of May, 2004, at Burlington, Vermont.

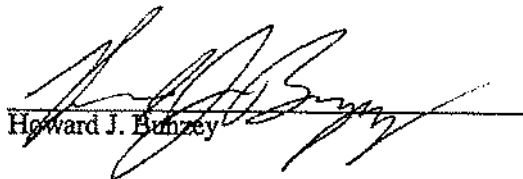

Howard J. Bunzey

Exhibit A

REDACTED**Employee Guide**

Last Changed on 03/11/2002 10:35:53 AM by Amy Kakalec/BVT/IDX1

Chapter #:	4	Chapter:	IDX STANDARDS AND RELATED POLICIES
		Section:	Information Technology Policies
		Topic:	Data Protection

THIS GUIDE IS NOT A CONTRACT. THE STATEMENTS CONTAINED ON THIS PAGE ARE SUMMARIES OF THE COMPANY'S POLICIES. FOR A COMPLETE WRITTEN COPY OF ANY POLICY, CONTACT THE HUMAN RESOURCES DEPARTMENT. IDX POLICIES ARE SUBJECT TO CHANGE AT ANY TIME FOR ANY REASON.

It is the responsibility of every employee to protect IDX confidential information.

Virus Policy

Each employee must adequately protect and defend his or her system(s) and information from unintended or malevolent destruction, and take reasonable steps to prevent the spread of malicious programs and computer viruses.

- Employees must not willfully introduce virus-infected files or media into the organization.
- Incoming information and media should be scanned for viruses before use.
- Employees must use and maintain approved virus-scanning software on their PC and any other system for which they are primarily responsible, including PCs used at home for IDX business purposes.
- Employees must not use software of unknown or questionable origin.

Data Preservation

Employees may not view or change information that they are not authorized to access or modify. Employees must take all reasonable steps necessary to prevent disclosure of information to anyone within or outside of the company who is not authorized to access it.

Adequate backup copies of all information must be made and kept safe, with the frequency of backup consistent with the value of the information and difficulty of recreating it.

IDX 001435

2/5/2003

Bunzey Decl. Page 4
CV03-1158P

Each employee is responsible for safeguarding data that is removed from the company premises for business purposes. This includes information on paper, magnetic media, and any PC or other electronic device that is taken on a business-related trip or to work at home. Information Systems and your manager must be notified immediately of any loss or theft of IDX information.

Disposal

Appropriate procedures must be followed when discarding sensitive or confidential information.

Paper documents must be shredded. Magnetic media must be erased and/or destroyed.

IDX 001436

2/5/2003

Bunzey Decl. Page 5
CV03-1158P

CONFIDENTIAL - 5 U.S.C. § 552

REDACTED



Employee Guide

Last Changed on 08/11/2002 10:34:44 AM by Amy Kakaiec/BVT:IDX1

Chapter #:	4	Chapter:	IDX STANDARDS AND RELATED POLICIES
		Section:	Information Technology Policies
		Topic:	Information Technology Resource Usage

THIS GUIDE IS NOT A CONTRACT. THE STATEMENTS CONTAINED ON THIS PAGE ARE SUMMARIES OF THE COMPANY'S POLICIES. FOR A COMPLETE WRITTEN COPY OF ANY POLICY, CONTACT THE HUMAN RESOURCES DEPARTMENT. IDX POLICIES ARE SUBJECT TO CHANGE AT ANY TIME FOR ANY REASON.

All hardware, software, computer supplies and documentation, telephone equipment and communications infrastructure has been purchased by and for the benefit of IDX, and must not be removed from the company without proper authorization. Each employee is responsible for the proper care and use of Information Technology (IT) resources.

Policy Statements

- All information technology resources must be used in accordance with all IDX policies.
- IT resources may not be used for personal gain.
- IT resources may not be used for entertainment.
- Installation and use of personal software on IDX systems is not allowed.
- IDX reserves the right to inspect, monitor, audit, review and record the contents and usage of any or all of its IT resources and environment.
- All information stored by employees at IDX, whether on paper, represented electronically, or in any other form, is by default viewable by company officials. IDX reserves the rights to view, copy, and delete any information contained on all IDX computing facilities, including servers and Personal Computers.
- Only systems owned by IDX may be used to connect remotely to the IDX Network. Failure to comply with this policy may result in the loss of remote access privileges.

IDX 001437

2/5/2003

Bunzey Decl. Page 6
CV03-1158P

CONFIDENTIAL - 5 U.S.C. § 552

REDACTED



Employee Guide

Last Changed on 08/11/2002 10:32:02 AM by Amy Kakalec/BVT (IDX)

Chapter #:	4	Chapter:	IDX STANDARDS AND RELATED POLICIES
		Section:	Information Technology Policies
		Topic:	Internet Usage

THIS GUIDE IS NOT A CONTRACT. THE STATEMENTS CONTAINED ON THIS PAGE ARE SUMMARIES OF THE COMPANY'S POLICIES. FOR A COMPLETE WRITTEN COPY OF ANY POLICY, CONTACT THE HUMAN RESOURCES DEPARTMENT. IDX POLICIES ARE SUBJECT TO CHANGE AT ANY TIME FOR ANY REASON.

IDX provides equipment, systems, and facilities for accessing the Internet and the World Wide Web.

The Internet is considered an unregulated public exchange. Employees must protect IDX and all its assets, including the confidentiality and sensitivity of corporate information, when conducting business on the Internet. Internet transmission capacity, commonly known as "bandwidth", is a shared company resource and it is the responsibility of every employee to use it appropriately.

Usage Policies

The Internet must be used in accordance with all other IDX policies.

Internet users must abide by all software licensing agreements, copyright laws, intellectual property and trademark laws, and any other applicable regulations.

Internet users may access only those systems, services or information which they are authorized to access. Confidential or sensitive information of any kind may not be sent via the Internet unless encrypted.

The primary purpose of the IDX Internet connection is to conduct company business. Occasional personal use is permitted, but must adhere to the following guidelines:

- Cost associated with the use is insignificant.
- Use is infrequent and of short duration.
- Use does not interfere with the employee's work
- Use does not negatively impact anyone else.

IDX 001439

2/5/2003

Bunzey Decl. Page 7
CV03-1158P

The following activities are strictly forbidden at all times:

Internet Use for Private or Personal Gain. Do not use the Internet for personal gain, including advancing or developing a personal business or product (including advertising or selling non-company products), gambling, excessive buying and selling of stocks (day trading), and job hunting.

Inappropriate Language. Accessing, creating, transmission of, printing or downloading material that is derogatory, defamatory, obscene, threatening, or offensive, such as slurs, epithets, or anything that may be construed as harassment or disparagement is prohibited.

Illegal Acts. This includes copyright infringement and software piracy, chain letters, and pyramid schemes.

Breaches of Company Security. Obey all security policies, including those pertaining to unauthorized distribution of data and information.

Interference. Do not attempt to disrupt other users, services or equipment.

Solicitation. This includes promoting religious, non-profit and political causes.

Misrepresentation. Never send, post or email personal comments that may be mistaken as the position of the company.

Pornography. Access or sending of sexually oriented messages or images of any kind is prohibited.

Unauthorized Access. Never access or attempt to access protected Internet resources without proper permission of the owner.

Instant Messaging. IDX has chosen Lotus' Sametime as the corporate internal and external instant messaging platform. Installation and use of 3rd party instant messaging software or tools is prohibited.

Streaming Media. Users should not stream non-business related audio and video from the Internet. Doing so is a waste of IDX's limited Internet bandwidth.

Gaming and Gambling. Online gaming and gambling are strictly prohibited.

Circumventing Security Precautions. Security precautions have been put in place to ensure that the data on the corporate network remains safe and accessible. Under no circumstances should users attempt to evade or circumvent any of these measures.

If there are questions about a use or activity that is not specifically mentioned in this policy, please contact the Information Systems Department or Legal Department for clarification.

IDX 001440

2/5/2003

Bunzey Decl. Page 8
CV03-1158P

Monitoring and Management

IDX may monitor usage of the Internet by employees, including reviewing a list of sites accessed by an individual. No individual should have any expectation of privacy in terms of their usage of the Internet. In addition, the Company may restrict access to certain sites that it deems are not necessary for business purposes.

Employees are prohibited from encrypting files on their computers or taking any other steps to block access to data or records, or conceal their activities, other than the methods provided by the Information Systems Department.

Protection of IDX from Public Internet Users

All IDX computing systems which will be accessed by non-IDX personnel must be inspected by Information Systems and approved by the appropriate Information Systems manager, and must implement the necessary safeguards to maintain information security. Internet users must report all security problems to Information Systems and/or the corporate security administrator.

Guidelines

During Internet communications, act with the discretion appropriate for an IDX representative. When applicable, actively disclaim that you are speaking for the company using the phrase "The contents of this communication do not necessarily represent the views of IDX Systems Corporation" or a reasonable facsimile.

Information received or retrieved from the Internet should be considered suspect, and require validation before being used for business purposes. Standard quality controls should apply to all data files and executable code obtained from the Internet. Anything retrieved should be quarantined and checked for viruses and other contaminants before being used or placed into the corporate computing environment.

Do not use company credit cards to purchase goods via the Internet. Purchases must follow established procurement policies.

Practice acceptable Internet etiquette (commonly referred to as "netiquette"). For more information contact Information Systems.

Employees who use personal Internet access capabilities or personal Internet Service Provider (ISP) accounts to perform IDX related business activities must adhere to the same guidelines that govern use of the IDX Internet connection, as well as all organizational resources.

This policy applies to all current and future Internet access methods, protocols and utilities

IDX 001441

2/5/2003

Bunzey Decl. Page 9
CV03-1158P

including, but not limited to, http, ftp, and telnet.